REMARKS

Claims 9-28 are presently pending in this application. In an office action mailed January 30, 2003 (Paper No. 6), claims 1-21 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,163,772 granted to Kramer et al. (hereinafter "*Kramer*"). This rejection is respectfully traversed.

Kramer fails to provide a basis for the rejection of claims 9-21 under 35 U.S.C. 102(e), as it fails to disclose each element of the claimed invention. For example, claim 9 includes "An apparatus for transmitting credit transaction data over a communications medium comprising: a protocol translator receiving the credit transaction data from one or more point of sale systems according to a transmission protocol; and an encryption system coupled to the protocol translator, the encryption system receiving the credit transaction data from the protocol translator and encrypting the credit transaction data." In contrast, *Kramer* discloses "An Authorization/Data Capture Module 1560 processes the requests originated by the merchant or the consumer and routes them to a Protocol Module 1565. Protocol Module 1565 is ***responsible for building a payment protocol request packet*** 1570 (e.g., an SSL-encapsulated ISO 8583 packet) ***before sending the request to a Gateway*** 1579. Gateway 1579 then awaits a response from Protocol Module 1565, and upon receiving the response, Gateway 1579 parses the data and provides unwrapped data to Authorization/Data Capture Module 1560. Authorization/Data Capture Module 1560 analyzes the response and updates a Transaction Log 1580. Transaction Log 1580 includes information concerning any successfully completed transactions and the accumulators or the transaction totals. The vPOS terminal creates and maintains Transaction Log 1580, and vPOS Configuration Data 1585 includes information that is used to configure. the behavior of the vPOS. The entire vPOS functionality is thread-safe and hence using the vPOS in a multi-threaded environment does not require any additional interfacing requirements." Thus, the protocol module 1565 of *Kramer* does not receive "the credit transaction data from one or more point of sale systems according to a transmission protocol," but instead ***builds a payment protocol request packet . . . before sending the request to a Gateway***. There is no suggestion in *Kramer* that the point-of-sale systems may have different transmission protocols, and in fact, only one transmission protocol is disclosed in *Kramer* – the ***payment protocol request packet***.

Claim 11 further includes a management system interface coupled to the protocol translator, the management system interface storing a protocol module to the protocol system. *Kramer* does not disclose any such management interface, nor that a protocol module can be stored to a protocol system. For example, *Kramer* states that protocol module 1565 is responsible for building a payment protocol request packet 1570 (e.g. an SSL-encapsulated ISO 8583 packet), but it does not disclose a management system interface storing a protocol module to the protocol system. In one exemplary embodiment, such a management system interface would be useful in a system having a large number of hubs with associated with point-of-sale card readers, where a new protocol module needs to be distributed to allow the hubs to interface with a new type of point-of-sale device. *Kramer* would have no need for such functionality, as it discloses virtual point of sale terminals that are all emulated from a common source. In the system of *Kramer*, there would be no need for a protocol system, much less for storing a protocol module to the protocol system.

Claim 12 includes a management system interface coupled to the encryption system, the management system interface storing an encryption module to the encryption system. *Kramer* teaches away from such functionality at col. 64, lines 32-44, where it is stated that the "architecture described here ensures that the single version of vPOS, no matter how it configured with extended terminal transaction interfaces, ***cannot be used to communicate any data other than that contained in the extended SET messages that have been approved for export by the U.S. Department of Commerce***. . . " (*emphasis added*). In contrast, the management system interface storing an encryption module to the encryption system allows the encryption module to be constantly updated if desired, such as to defeated attempts to "hack" the encryption.

Claim 13 includes "a method for transmitting credit transaction data over a communications medium comprising: receiving credit transaction data from two or more point of sale devices, each reading credit card data from a magnetic stripe of a credit card; determining a point-of-sale device data transmission protocol to use to assemble the credit transaction data into an authorization request; encrypting the authorization request; transmitting the encrypted authorization request over the communications medium; decrypting the encrypted authorization request; determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and transmitting the authorization request to the appropriate authorization system." *Kramer* fails to disclose point of sale devices reading credit card data from a magnetic stripe of a credit card – instead, it addresses a system that facilitates virtual transactions, at which the consumer does not present a card to the merchant. As such, there is no need for *Kramer* to determine a point-of-sale device data transmission protocol to use to assemble the credit transaction data into an authorization request.

Claim 14 includes receiving the credit transaction data in accordance with one or more of an ISO 8583 protocol or a Visa-K protocol. *Kramer* fails to disclose point-of-sale protocols such as the Visa-K protocol, because it addresses a system that facilitates virtual transactions, at which the consumer does not present a card to the merchant. As such, *Kramer* does not even suggest a combination with such point-of-sale systems, but rather a system in which all transactions are virtual and do not require the card to be presented to the merchant.

Claim 17 includes a "method for controlling the transmission of credit transaction data comprising: transmitting one or more control messages to a remote hub; processing the control message at the remote hub; and performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message." Again, *Kramer* addresses a system that facilitates virtual transactions, at which the consumer does not present a card to the merchant, and there is no remote hub disclosed in *Kramer* that interfaces with point of sale devices that read magnetic card stripes.

New claim 22 includes a "system for transmitting credit transaction data comprising: two or more point-of-sale systems, each point-of-sale system using a proprietary data format to read credit card data from a magnetic stripe of a credit card and generate credit transaction data; a remote hub system coupled to a communications medium, the remote hub system receiving the credit transaction data from one or more point of sale systems, translating the credit transaction data from the proprietary data format to a predetermined data format, encrypting the translated credit transaction data, and transmitting the translated encrypted credit transaction data over the communications medium; and a gateway system coupled to the communications medium, the gateway system receiving the encrypted translated credit transaction data, decrypting the encrypted translated credit transaction data, and transmitting the translated credit transaction data to an authorization system."

All other claims not specifically addressed are believed to be allowable at least for the reasons that they depend from other allowable claims, and add limitations not found in the prior art.

CONCLUSION

In view of the foregoing remarks and for various other reasons readily apparent, Applicants submit that all of the claims now present are allowable, and withdrawal of the rejections and a Notice of Allowance are courteously solicited.

If any impediment to the allowance of the claims remains after consideration of this amendment, a telephone interview with the Examiner is requested by the undersigned at (214) 969-4669 so that such issues may be resolved as expeditiously as possible.

An additional fee of $110.00 is believed to be due for a one-month extension of time to respond, which is hereby petitioned for. A check for this amount has been included with this filing. No additional fee is believed to be required with this response. If any applicable fee or refund has been overlooked, the Commissioner is hereby authorized to charge any fee or credit any refund to the deposit account of Akin, Gump, Strauss, Hauer & Feld, L.L.P., No. 01-0657.

Respectfully Submitted,

Date: 5/30/03

Christopher J. Rourk, Reg. No.39,348
Akin, Gump, Strauss, Hauer & Feld, L.L.P.
P.O. Box 688
Dallas, TX 75313-0688
Tel. No.: (214) 969-2800
Fax No.: (214) 969-4343

ATTORNEY FOR APPLICANTS